OKRUGLI STO
„Digitalna forenzika i IT veštačenje u funkciji borbe protiv visoko tehnološkog kriminala“

WIRELESS FORENZIKA

Prof. dr Dragana Bečejski-Vujaklija
Fakultet organizacionih nauka, Beograd

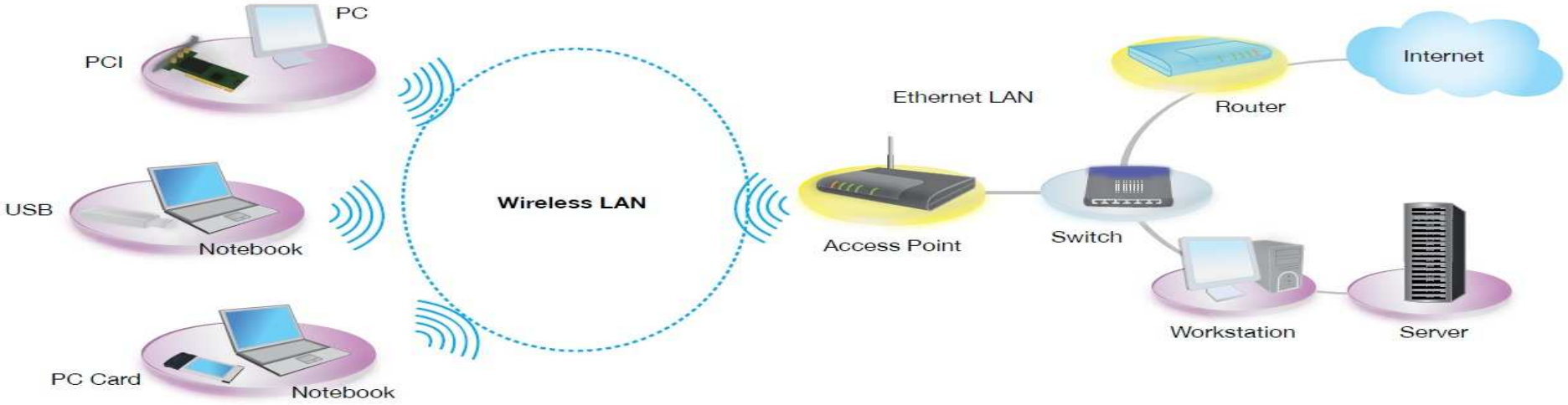
WIRELESS FORENZIKA – sadržaj izlaganja

- Osnovni pojmovi i vrste bežičnih mreža
- Bezbednost i zaštita u bežičnim mrežama
- Napadi na bežične mreže
- **Forenzika u bežičnim mrežama**
  - **postupci**
  - **alati**

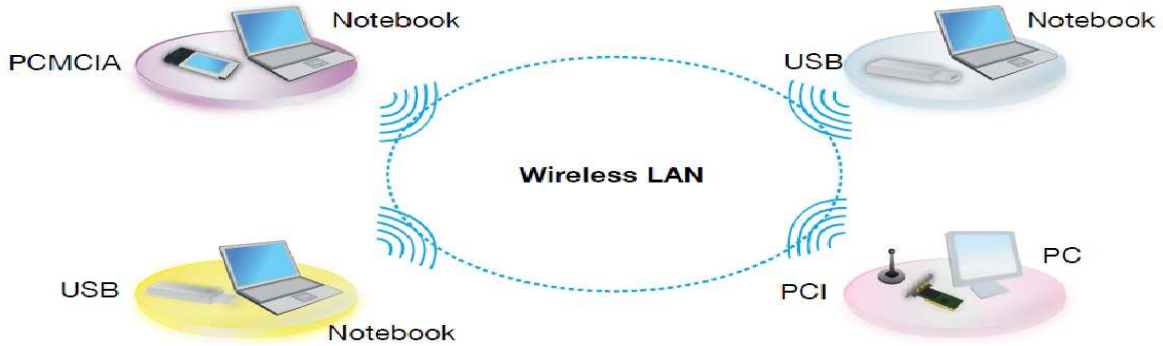
Forenzika u bežičnim mrežama

- “Forenzika u bežičnim mrežama (eng. *wireless forenzics*) je grana kompjuterske forenzike, koja predstavlja postupak utvrđivanja činjenica primenom odgovarajućih metoda nad digitalnim medijima, a u svrhu korišćenja u sudskom postupku.”
- Termin „*wireless forenzics*“ prvi je upotrebio stručnjak za kompjutersku sigurnost *Marcus J. Ranum* 1997. godine, za metode i alate za prikupljanje i analizu prometa u bežičnim kompjuterskim mrežama, na način koji omogućava njihovu primenu u sudskom postupku.

Infrastrukturna bežična mreža

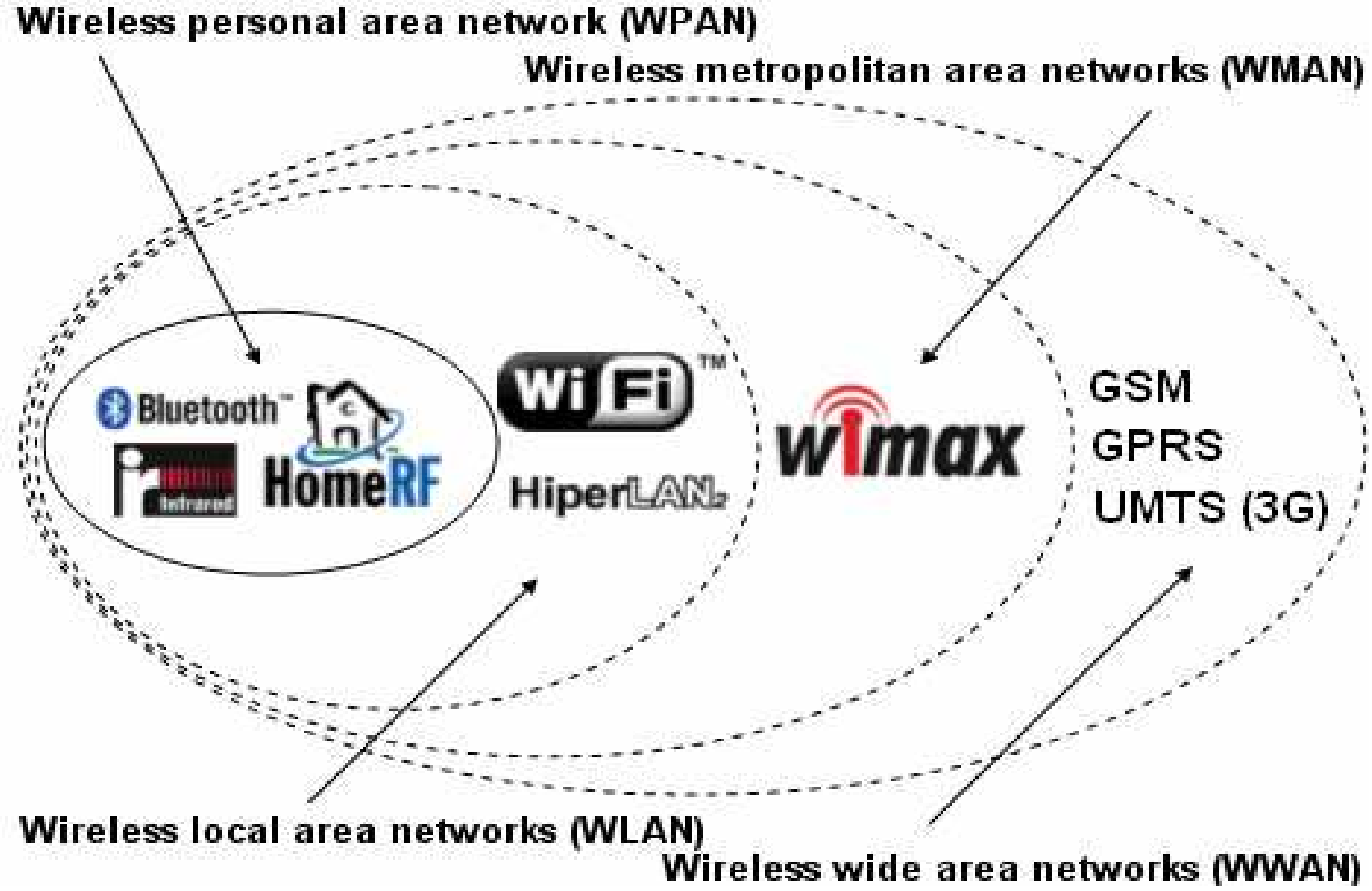


Ad-hoc bežična mreža



Vrste Wireless mreža

- **Bežične mreže na daljinu** (*Wireless Wide Area Network – WWAN*), pokrivaju relativno velike geografske prostore i koriste radio i satelitske linkove. Koriste se za pokrivanje univerzitetskih centara i gradova. Fleksibilnije, jednostavnije za instaliranje i održavanje, i jeftinije po ceni priključka nego tradicionalne žične mreže.
- **Lokalne bežične mreže** (*Wireless Local Area Network – WLAN)* omogućavaju da računari na jednoj geografskoj lokaciji dele informacije i zajedničke uređaje (štampači, baze podataka, itd.).
- **Personalne ili lične mreže** (*Personal Area Network – PAN)* omogućavaju komunikaciju prvenstveno elektronskih uređaja unutar prostora od nekoliko metara i razmenu komunikacionih i sinhronizacionih informacija. Koriste infracrvene talase (*infrared*) i *bluetooth*.


Wireless personal area network (WPAN)
Wireless metropolitan area networks (WMAN)
Bluetooth
HomeRF
Wi Fi
HiperLAN
wimax
GSM
GPRS
UMTS (3G)
Wireless local area networks (WLAN)
Wireless wide area networks (WWAN)

Ciljevi WLAN bezbednosti

- **Poverljivost:** jaka zaštita poverljivosti podataka; pravo čitanja između dva legitimna WLAN čvora dati samo autorizovanim korisnicima.
- **Integritet:** detektovanje bilo kakve promene na podacima u tranzitu, bile one namerne ili slučajne.
- **Dostupnost:** WLAN i pripadajući resursi treba da budu dostupni svim pojedincima i uređajima na zahtev.
- **Kontrola pristupa:** ograničiti prava pojedinaca i uređaja za pristup mreži i njenim resursima. Veze između WLAN čvorova uspostaviti i verifikovati pomoću jake uzajamne autentifikacije.

Striktno sprovođenje bežične sigurnosne politike:

- Edukacija korisnika
- Zabrana korišćenja nezavisnog "Ad hoc" moda
- Zabrana postavljanja neautorizovanih pristupnih tačaka "rogue access point"
- Gašenje pristupne tačke kada se ne koristi
- Redukcija ili zabrana korišćenja aplikacija koje koriste veliki prenosni pojas za slanje poverljivih podataka
- Istraživanje i izbor proizvoda sa najboljom sigurnosnom strategijom i dugovečnošću na tržištu
- Provera i periodično ispitivanje sigurnosnih pretnji.

Najčešći napadi na bežične mreže (1)

- **Pasivni napadi –neautorizovani korisnik dobija pristup informaciji, pri čemu ne menja njen sadržaj**.
  - **Prisluškivanje** – Napadač prati prenos sadržaja poruke. (sluša prenos između radnih stanica ili upada u prenos između bežičnog uređaja i bazne stanice).
  - **Analiza prometa** – Napadač dobija poverljive podatke prateći prenos uzoraka komunikacije.
- **Aktivni napadi –neautorizovani korisnik modifikuje poruku, tok podataka ili datoteku. Ovaj tip napada je moguće detektovati, ali nekad ga je nemoguće izbeći.**
  - **Maskiranje** – Napadač se pretvara da je autorizovani korisnik i tako dobija određene neautorizovane privilegije.
  - **Odgovor** – Napadač prati prenos (pasivni napad) i šalje poruke kao legitimni korisnik.
  - **Modifikacija poruke** – Napadač menja legitimne poruke brisanjem, dodavanjem, menjanjem ili promenom redosleda.
  - **Uskraćivanje računarskih resursa** – Napadač sprečava ili zabranjuje regularnom korisniku upravljanje svojstvima komunikacije.

Najčešći napadi na bežične mreže (2)

- Lociranje bežičnih mreža - samo po sebi nije napad, ali vrlo lako kasnije može dovesti do napada

  (da bi neko mogao napasti bežičnu mrežu, prvo mora da sazna gde se ona i koje su joj karakteristike).
- *War Driving* - skeniranja područja korišćenjem prevoznog sredstva. Može skenirati područje celog grada u veoma kratkom roku.

  Napredni War Driveri koriste GPS i dobijene rezultate odmah ucrtavaju u mapu.

Zaštita u bežičnim mrežama

- Pomoću istih alata koje koriste hakeri da prodru do mreže, možemo pronaći bezbednosne rupe, što će nam pomoći pri zaštiti sistema.

Proces bežične forenzike

Proces bežične forenzike podrazumeva

1. prikupljanje svih podataka koji se prenose preko mreže
2. analiziranje mrežnih događaja kako bi se
   - otkrile anomalije mreže,
   - otkrili izvori bezbednosnih napada,
   - istražile povrede na računarima i bežičnim mrežama,
   - utvrdilo da li su u pitanju nezakonite i neovlašćene aktivnosti.

Istraživanje WLAN-a u cilju prikupljanja forenzičkih dokaza

- Prvi korak je utvrđivanje komponenti sumnjive bežične mreže, kao i da li su komponente autorizovane ili nisu.
- Bežični hardver može biti smešten svuda gde postoji izvor napajanja (zidovi, police, ormani itd.)
- Potražiti pripadajuća dokumenta, instalacione diskove i sve prateće stavke vezane za WLAN uređaje.

Identifikovanje digitalnih komponenata

- U slučaju aplikacija, potražiti drajvere i instalacije programa koji su povezani sa wireless sistemima, posebne alatke za monitoring, bežično snimanje kao i poznate hakerske alate.
- U okviru operativnog sistema, pored drajvera, treba potražiti linkove ili prečice ka mreži i deljenju mrežnih resursa, kao i ispitati *registry* bazu u cilju indikacije bežičnih uređaja ili veze.
- Svaki bežični uređaj u WLAN-u sadrži različite vrste dokaza i treba da se tretira zasebno pri prikupljanju dokaza, a potom prikupljene podatke treba kumulativno uporediti u fazi analize.

Tehnički izazovi za prikupljanje WLAN podataka

- Prilikom izbora forenzičkog alata potrebno je osigurati da on podržava isti komunikacioni standard kao i onaj koji koristi mreža koju je potrebno nadzirati.

- Forenzički programski paketi koriste posebnu tehniku pretraživanja celog frekvencijskog spektra koji posmatramo i uzimanja uzoraka svih raspoloživih kanala.

  (uobičajena bežična oprema sadrži samo jednu radio komponentu i omogućava komunikaciju na samo jednom kanalu)

Problem pokretljivosti klijenata

- Jedna od glavnih prednosti bežičnih mreža je mogućnost kretanja računara unutar nje bez prekida veze na mreži. Ovo otežava zadatak sprovođenja forenzičke analize mrežnog prometa.
- Rešava se postavljanjem višestrukih uređaja za snimanje prometa na različitim položajima unutar područja koje se nadzire.

Karakteristike uređaja za prikupljanje prometa

- Bežičnu forenziku je moguće sprovoditi korišćenjem standardne PC opreme i programskih paketa otvorenog programskog koda
- Za izgradnju računarskog sisitema koji zadovoljava sve zahteve potrebna je relativno skupa oprema i implementacija.
- Velika propusna moć sabirnica koje međusobno povezuju bežične mrežne kartice
- Velika propusna moć memorijskih sabirnica
- Interfejs hard diskova, kako ne bi došlo do zagušenja i gubitka potencijalnih dokaznih materijala
- Optimalni kapaciteti za skladištenje velikih količina podataka karakterističnih za bežičnu forenziku

Alati za zaštitu

- WLAN alati za otkrivanje
  - Netstumbler — Verzije za Windows i Linux
  - Kismet — Linux
  - MacStumbler — Mac OS
  - MiniStumbler — Pocket PC
  - Mognet — Java
- Wireless network sniffers
  - AiroPeek — Windows
  - AirTraf — Linux
  - Ethereal — All OSs
  - Sniffer Wireless — Windows i Pocket PC
  - BSD AirTools — BSD

WEP alati za razbijanje

- WEPCrack — Linux
- AirSnort — Linux
- BSD-Tools dweputils — BSD
- AirCrack — Linux i Windows

Komercijalni i open source alati

- Skup alata korišćenih za forenzičku analizu mrežnog prometa naziva se NFAT (eng. *Network Forenzic Analysis Tool*). Najpoznatiji komercijalni alati namenjeni forenzičkoj analizi žičanih mreža su *„Sandstorm NetIntercept“*, *„Niksun NetVCR“* i *„eTrust Network Forensics“* alati.
- Open source programski paketi:
  - **Wireshark** je alat s grafičkim korisničkim interfejsom koji omogućuje detaljnu analizu polja prikupljenih paketa podataka,
  - **ngrep** (eng. *Network Global Regular Expression Parser*) omogućuje traženje specifikovanih znakova u paketima podataka,
  - **tcdump** i **tshark** su alati za stvaranje skripti sa tekstualnim grafičkim interfejsom, a namenjeni su automatizaciji pojedinih analitičkih zadataka kao što je filtriranje prikupljenog prometa prema postavljenim kriterijumima.

Specifični Alati

- Janus Project je komercijalni alat, predstavljen 2006. godine, koji sadrži 8 wireless kartica za skeniranje, prikupljanje podataka i krekovanje enkripcija.
- WLAN-14 je baziran na Linux operativnom sistemu, dizajniran kao komercijalni uređaj za bežičnu forenziku. Omogućava bezbedno prikupljanje 802.11 b/g bežičnih podataka. Poseduje 15 bežičnih kartica, GPS, priključak za eksternu antenu i podršku za hot-swap diskove.

Postupci i preporuke za korišćenje forenzičkih alata (1)

- Forenzički alat treba da prikuplja sav promet, bez filtriranja, kako analizi ne bi promakli pojedini bežični uređaji prisutni na mreži. Kasnije, tokom analize, moguće je koristiti filtere, zbog ubrzavanja postupka.
- Forenzički alat treba da bude potpuno pasivan, tj. da ne odašilje pakete. Ovo se postiže
  - na sistemskom nivou, korišćenjem atenuatora koji redukuje ili sasvim otkazuje prenos snage, korišćenjem jednosmernih pojačala
  - na programskom nivou, postavljanjem mrežne kartice u nadzorni način rada.
- Korišćenje uređaja sa 15 radio komponenti ili kartica kako bi se mogli nadgledati svi kanali i istovremeno pretraživati radio spektar u potrazi za novim mrežama.
- Korišćenje GPS sistema za navigaciju – pruža precizne oznake za utvrđivanje mesta i vremena prikupljanja dokaza. U logove treba beležiti intervale sinhronizacije uređaja sa GPS satelitima (kako bi bilo moguće dokazati da su očitavanja tačna).

Postupci i preporuke za korišćenje forenzičkih alata (2)

- Uređaj za prikupljanje prometa može biti na nepristupačnom mestu. Tada je potrebna mogućnost udaljenog pristupa uređaju, pomoću zasebnog sistema, koji treba dobro zaštititi autentikacijskim i enkripcijskim mehanizmima, kako ne bi bio kompromitovan.
- Treba koristiti uređaje na koje je moguće priključiti spoljašnju antenu sa ciljem povećanja osetljivosti prijemnika.
- Za procenu udaljenosti osumnjičenog od forenzičkog uređaja, vršiti prikupljanje podataka o snazi signala.
- Preporučeno je korišćenje uređaja (mrežnih kartica i radio komponenti) sa velikom osetljivošću prijemnika, kako prikupljanje paketa ne bi bilo prekinuto u slučaju pogoršanja uslova rada.
- Kako bi se omogućila rekonstrukcija postupaka forenzičkog alata, što može biti potrebno tokom sudskog procesa, savetuje se korišćenje naprednih mogućnosti stvaranja logova.

Analiza bežičnog prometa

- Standardni postupci analize kod žičanih i bežičnih mreža
  - normalizacija podataka, tzv. rudarenje podataka (eng. *data mining*), koje omogućava jednostavno pretraživanje prikupljenog prometa,
  - prepoznavanje uzoraka, kako bi se otkrile anomalije i sumnjivi uzorci,
  - analiza protokola, koja je važna za razumevanje različitih zaglavlja pojedinih protokola
  - rekonstrukcija aplikacionih sesija
- Specifičnosti bežične forenzike odnose se na:
  - spajanje prometa više kanala,
  - rukovanje prometom preklapajućih kanala,
  - filtriranje i
  - ubrzavanje analize.

Zaključak

- Bežične tehnologije će u budućnosti nalaziti primenu na sve širim područjima i u sve većem obimu.
- Sigurno je da će znatan broj primena biti zlonamerne prirode.
- U tom kontekstu očigledna je važnost i nužnost odgovarajućih metoda forenzičke analize u postupcima otkrivanja i analize sigurnosnih incidenata.
- Osnovni zadatak forenzičke analize bežične mreže je prikupljanje ukupnog ostvarenog prometa.
- Traje „trka u naoružanju“ između zlonamernih korisnika i stručnjaka za sigurnost, pa je potrebno stalno školovanje kadrova i ažuriranje korišćenih alata.

Zahvalnost

- Aleksandaru Božikiću, studentu master studija na FON-u, modul IT menadžment, za obavljeno istraživanje i prikupljene podatke iz oblasti Wireless forenzike

Korisni izvori

- Firma “Data Solution”
  www.datasolutions.rs/srp/kompjuterska-forenzika/kompjuterska-forenzika-osnove.htm
- Uvod u računalnu forenziku, Materijali za studente, Fakultet elektrotehnike i računarstva Zagreb, www.fer.hr/_download/repository/03_Ieee_Uvod_u_racunalnu_forenziku.pdf
- Dr Mirjana Drakulić, mr Ratimir Drakulić "Izazovi Cyber prostora - Cyber forenzika", Časopis Internet ogledalo br.56